[Billing Code: 6750-01P]

FEDERAL TRADE COMMISSION

Public Workshop:

Proof Positive: New Directions for ID Authentication

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice Announcing a Two-Day Public Workshop and Requesting Public Comment and Participation.

SUMMARY: The FTC and other participating agencies are planning to host a two-day public workshop to explore the role of authentication processes in preventing identity theft. The workshop will provide a forum for discussion among public sector, private sector, and consumer representatives about better ways to authenticate the identities of individuals.

DATES: Workshop, *Proof Positive: New Directions for ID Authentication*, will be held on April 23, 2007 from 8:30 a.m. to 5:00 p.m. and April 24, 2007, from 8:30 a.m. to 12:30 p.m., in the Federal Trade Commission's Satellite Building Conference Center located at 601 New Jersey Avenue, N.W., Washington, DC. The events are open to the public and attendance is free of charge. There will be no pre-registration.

Participants: As discussed below, written requests to participate as a panelist in the workshop must be filed on or before March 9, 2007. Persons filing requests to participate as a panelist will be notified on or before March 23, 2007, if they have been selected to participate.

Comments: Whether or not selected to participate, persons may submit written comments on the issues and topics set out below. Such comments must be filed on or before March 23, 2007.

ADDRESSES: Interested parties are invited to submit requests to participate and comments in accordance with the following instructions:

Requests to Participate as Panelist in Workshop:

Parties seeking to participate as panelists in the workshop must notify the FTC in writing of their interest in participating on or before March 9, 2007. Requests to participate as a panelist should be captioned "ID Workshop – Request to Participate, P075402" and may be submitted by any of the following methods. However, if the request contains any material for which confidential treatment is requested, it must be filed in paper form, and the first page of the document must be clearly labeled "Confidential."[1]

- E-mail: Requests to participate can be submitted electronically to: idmworkshop@ftc.gov.
- Mail or Hand Delivery: A request to participate filed in paper form should include "ID Workshop, P075402," both in the text and on the envelope and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H-135 (Annex N), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Because paper mail in the Washington area and at the Commission is subject to delay, please consider submitting your request by email, as prescribed above. The FTC is requesting that any request

[1] Commission Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. See Commission Rule 4.9(c)), 16 CFR 4.9(c)).

filed in paper form be sent by courier or overnight service, if possible.

Parties should include in their requests a statement setting forth their expertise in or knowledge of the issues on which the workshop will focus and their contact information, including a telephone number, facsimile number, and email address (if available), to enable the FTC to notify them if they are selected.

FTC staff will select a limited number of panelists to participate in the workshop, using the following criteria.

1. The party has expertise in or knowledge of the issues that are the focus of the workshop;
2. The party's participation would promote a balance of interests being represented at the workshop; and
3. The party has been designated by one or more interested parties (who timely file requests to participate) as a party who shares group interests with the designator(s).

The FTC will notify panelists on or before March 23, 2007, as to whether they have been selected. The number of parties selected will not be so large as to inhibit effective discussion among them. For those not serving as panelists, there also will be time during the workshop to ask questions.

Comments

The FTC requests that interested parties submit written comments on the issues raised below. Studies, surveys, research, and empirical data are especially useful. Comments should be captioned "ID Workshop – Comment, P075402" and must be filed on or before March 23, 2007. If the comment contains any material for which confidential treatment is requested, it must be

filed in paper form, and the first page of the document must be clearly labeled "Confidential."[2] Otherwise, comments may be submitted by any of the following methods.

- Electronic Filing: Comments filed in electronic form should be submitted by clicking on the following Web link: https://secure.commentworks.com/ftc-idmworkshop and following the instructions on the Web-based form. To ensure that the Commission considers an electronic comment, you must file it on the Web-based form at https://secure.commentworks.com/ftc-idmworkshop.
- Mail or Hand Delivery: A comment filed in paper form should include "ID Workshop, P075402," both in the text and on the envelope and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H-135 (Annex N), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Because paper mail in the Washington area and at the Commission is subject to delay, please consider submitting your comments in electronic form, as prescribed above. The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be

[2] Commission Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. See Commission Rule 4.9(c), 16 CFR 4.9(c).

considered by the Commission and will be available to the public on the FTC Web site, to the extent practicable, at http://www.ftc.gov/os/publiccomments.htm. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at http://www.ftc.gov/ftc/privacy.htm.

FOR FURTHER INFORMATION CONTACT: Stacey Brandenburg, Joanna Crane, or Naomi Lefkovitz at (202)-326-2252.

SUPPLEMENTARY INFORMATION:

Background and Proposed Agenda

Identity theft takes many forms and is committed for various purposes, including financial gain, avoidance of criminal penalties, and facilitating criminal activity (e.g., opening new credit accounts or draining bank accounts, evading criminal arrest warrants, and facilitating terrorist activities). But in its most basic form, it is a crime of deception relying on the unauthorized use of identifying information or credentials of another individual. At present, many transactions that depend on correct identification are conducted either remotely, or if in person, between individuals who are strangers. Because such transactions necessarily rely on an individual's use of identifying information or credentials in order to prove his or her identity, there is a potential risk of identity theft. Thus, the ability to determine when an individual is not who he or she purports to be is an important key to preventing identity theft.

The Identity Theft Task Force ("Task Force") was established by Executive Order of the President on May 10, 2006. The Order directed the Task Force to deliver a strategic plan to the

President on the federal government's response to identity theft. The Task Force, which is chaired by the Attorney General and co-chaired by the Chairman of the FTC, delivered an interim set of recommendations on September 19, 2006 that included the recommendation to hold a workshop focused on promoting improved means of authenticating the identities of individuals.[3]

To implement the Task Force's recommendation and to begin greater study of this area, the FTC and other Task Force agencies[4] will hold a workshop to explore the means by which identity theft can be prevented through better authentication of individuals.[5] The workshop will facilitate a discussion among public sector, private sector, and consumer representatives and will focus on technological and policy requirements for developing better authentication processes, including the incorporation of privacy standards and consideration of consumer usability.

---

[3] President's Identity Theft Task Force Summary of Interim Recommendations (2006), *available at* http://www.ftc.gov/opa/2006/09/idtheft.htm.

[4] For a list of the agencies comprising the Task Force, *see* Executive Order: Strengthening Federal Efforts to Protect Against Identity Theft (2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.

[5] The term "authentication" generally means the process of ensuring that an individual is who she or he claims to be. However, this process is more easily understood as comprising two distinct steps. The first step is the identification of an individual at the onset of the relationship between the individual and the verifying entity (e.g., an individual's identity will be verified when he or she applies for a passport or opens a financial account). The second step is the reaffirmation that the individual is the same individual whose identity was initially verified (e.g., the individual's passport is checked when he or she travels in or out of the country or the individual provides a password or other credentials to the financial institution when accessing an existing account). Although different terms can be applied to these steps, the first step is often labeled verification and the second step, particularly with respect to online environments, is often labeled authentication. For greater clarity, these distinctions are used in the invitation for comment section set forth herein.

To help in planning for the workshop, the FTC invites comments on ways to improve authentication processes in order to reduce the incidence of identity theft, including but not limited to, comments on the issues and topics set out below:

1. ESTABLISHING IDENTITY - UNDERSTANDING VERIFICATION PROCESSES

- In what ways can identities be established? How can individuals prove their identities when establishing them in the first instance?
- Please comment on the strengths and weaknesses of relying on traditional identification documentation or credentials such as birth certificates, Social Security cards, driver's licenses, and passports.
- Please comment on the strengths and weaknesses of new or emerging tools for establishing individuals' identities. Examples may include consumer information databases, which can be used to confirm whether a name and other personal information (e.g., Social Security number) belong together, and fraud detection software, which can be used to identify anomalous patterns or behaviors that may signal use of a false identity.
- What roles should the public sector or the private sector have in establishing identification credentials? Within the public sector, what roles should different levels of government (i.e., federal, state, local) have in establishing identification credentials?

2. CONFIRMING THE ESTABLISHED IDENTITY - CURRENT OR EMERGING USE OF AUTHENTICATION TECHNOLOGIES OR METHODS

- What are some current or emerging authentication technologies or methods (e.g., biometrics, public key infrastructure, knowledge-based authentication) for confirming established identities? Describe the contexts in which they may be used and their strengths and weaknesses.
- Please comment on the concept of multifactor authentication and how it is being or should be applied.
- To what extent are consumer information databases being used to authenticate individuals? One example of such use is to support knowledge-based authentication tools, which generate questions the answers to which only the consumer would know.
- To what extent do current or emerging authentication technologies or methods incorporate or rely on readily-available identification information, such as Social Security numbers? How might such reliance affect the risk of identity theft?
- To what extent do these technologies or methods meet consumer needs, such as ease of use? To what extent do these technologies or methods raise privacy concerns, including concerns about the tracking and profiling of an individual's movements or transactions by the public or private sector?

3. COMPARING VERIFICATION AND AUTHENTICATION SYSTEMS

- What are some of the different models for verification and authentication systems? Please comment on their strengths and weaknesses. For example, what

are the relative merits of a centralized identification system where a single or a limited number of organizations identify all individuals and issue credentials that other entities can rely upon versus a decentralized identification system where each organization develops its own procedures and separately verifies and authenticates the individuals with which it is involved?

- In considering the relative merits of different systems, please comment on:
    - Consumer acceptance and to what degree consumer education may facilitate such acceptance; and
    - Any privacy concerns including issues raised with respect to data collection, use, and storage.
- In addition to reducing identity theft, how might better systems or processes for proving claims of identity generate other consumer benefits (e.g., providing access to various commercial or government services)?
- How are other countries addressing verification and authentication issues, particularly as the issues relate to identity theft? What lessons can be learned?

4. UPCOMING CHALLENGES IN AUTHENTICATION

- As technologies converge to allow consumers to conduct financial or other sensitive transactions in new ways, how can appropriate authentication processes or technologies be incorporated to ensure that consumers receive the intended benefits of these advances without exposing them to new vulnerabilities?

By direction of the Commission.

Donald S. Clark
Secretary